

(43) 公表日 平成14年5月8日 (2002.5.8)

(51) Int.Cl.
H04L 12/46
12/28
12/18P.I.
HO 4 L 11/00
11/18
310 C

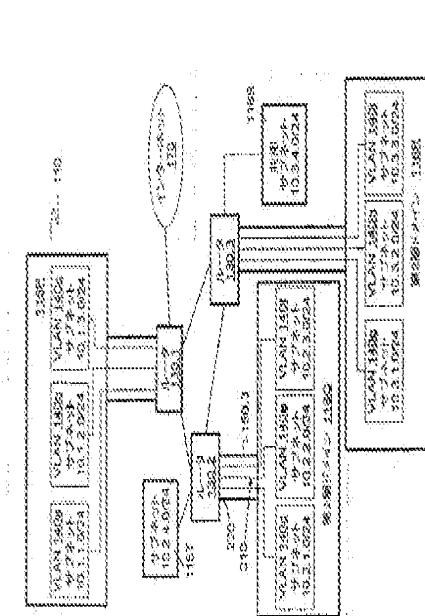
特許公報

発明の名稱	特願2000-546493(P2000-546493)	発明の名稱	特願2000-546493(P2000-546493)
(21) 出願番号	特願2000-546493(P2000-546493)	(71) 田嶋人 インターネットワーク・サービス・エイェス・エーボレインジョン	特願2000-546493(P2000-546493)
(22) 仕様日	平成11年4月22日 (1999.4.22)	Int'rnal Network Services Corporation	平成11年4月22日 (1999.4.22)
(23) 翻訳文提出日	平成12年10月12日 (2000.10.12)	アメリカ合衆国ワシントン州08101-4084・シダトル・スイート 1000・デンズ	アメリカ合衆国ワシントン州08101-4084・シダトル・スイート 1000・デンズ
(24) 國際出願番号	PCT/US99/08666	マクニール、トーマス・ジム・ストリート 601	マクニール、トーマス・ジム・ストリート 601
(25) 國際公開日	WO99/56436	(72) 田嶋人 アメリカ合衆国カリフォルニア州104097・オーレンム・ダイースト 1000ノース 1072	(72) 田嶋人 アメリカ合衆国カリフォルニア州104097・オーレンム・ダイースト 1000ノース 1072
(26) 優先日	09/067,761	(74) 代理人 大島 陽一	(74) 代理人 大島 陽一
(27) 優先権主張団	米国 (U.S.)		

(54) 【発明の概要】 ネットワークにおける接続の確立

(57) 【発明】

幾つかのドメイン (「第2層ドメイン」) を含む所定のネットワークが、ルータが、トライックルはMACアドレス (又は、他のデータリンク層アドレス) に基づき送信される。ルータは、IPアドレス又は他のネットワークアドレスに基づきトライックルの経路を指定する。ネットワーク管理者は、通信を許可されたサブネットワークの集まりである各接続ドリーブを指定する。また、管理者は、どのエンティティオブジェクトアドレス、ポート、又はユーティリティオブジェクトを指定する。そのエンティティオブジェクトは、同一のドメイニア内に存在し得る。エンティティオブジェクトアドレスは、ルータに対してアクセスリストを自動的に作成し、管理者の指定に従つてトライックルを許容又は拒否する。また、エンティティオブジェクトアドレスは、ルータに對してアクセス制御リストを自己更新する。ここで、各ドメインはドメイン内にドメイン全体である。各ドメインにおける接続性はVLANにより制限され、指定に従つてトライックルを許可する。



最終頁に續く

【特許請求項の範囲】

【請求項1】 ネットワーク端末をノードチャル間報道信ドメイン（VBDs）に接続するための方法であって、
ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネットワーク端末から受信する過程と、
1以上のVBDを含むユーザの属する接続グループを決定する過程と、
前記ネットワーク端末が接続される1以上のVBDを決定する過程であって、前記
1以上のVBDが前記接続グループのメンバーであるような前記決定過程と、
前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する
過程とを含むことを特徴とする方法。

【請求項2】 各VBDが、前記トライックが生じる前記VBDへの間報道信
トライックを制限可能なドメインのサブドメインであり、
前記接続グループが、少なくとも2つのドメインからのVBDを含み、
前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含
む前記ドメインに基づき決定されることを特徴とする請求項1に記載の方法。

【請求項3】 各VBDがVLANであり、また前記ネットワーク端末が、前記
接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接
続されることを特徴とする請求項2に記載の方法。

【請求項4】 ネットワーク端末をノードチャル間報道信ドメイン（VBDs）
に接続するための構造体であって、
ネットワーク上においてネットワーク端末のユーザを識別する情報を前記ネット
ワーク端末から受信する手段と、
1以上のVBDを含むユーザの属する接続グループを決定する手段と、
前記ネットワーク端末が接続される1以上のVBDを決定する手段であって、前記
1以上のVBDが前記接続グループのメンバーであるような前記決定手段と、
前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する
手段とを含むことを特徴とする構造体。

【請求項5】 各VBDが、前記トライックが生じる前記VBDへの間報道信
トライックを制限可能なドメインであり、

前記接続グルーブが、少なくとも2つのドライバからのVBDを含み、

前記ネットワーク端末が接続された以上にVBDが、前記ネットワーク端末を含む前記ドライバにに基づき決定されることを特徴とする請求項4に記載の構造体。
【請求項6】 簡VBDがVLANであり、また前記ネットワーク端末が、前記接続グルーブに属するVLAN並びに前記ネットワーク端末を含む前記ドライバに接続されることを特徴とする請求項5に記載

【請求項7】 前記構造体が、(1)所定のコンピュータシステム、及び(2)前記コンピュータシステムにコードされた所定のプログラムを含み、前記コンピュータシステム及び前記決定手段の各々を含むことを特徴とする請求項4に記載の構造体。

【請求項8】 前記構造体が、所定のコンピュータの記取り可能な媒体であり、そこで各手段が、1以上のコンピュータの命令、コンピュータの統取り可能なデータ、又は1以上の命令及びデータの組合せを含むことを特徴とする請求項4に記載の構造体。

【請求項9】 ネットワークドライバ間のトラフィックの経路を指定する以上的の装置に対するアセス制御リスト(ACL)を生成するための方法において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドライバ間においてどのようなトラフィックが許可及び／又は拒否されるかを決定し、更に、サブネットワークの各グループ内においてトラフィックが許可されるように、サブネットワークの1以上のグループを規定する過程であって、各サブネットワークがネットワークドライバの一部であるか、或いはネットワークドライバの全てであり、また各グループに対して、所定のコンピュータシステムに前記グループに属するサブネットワークの識別子を与えるような前記過程と、

前記コンピュータシステムが、各グループ内のトラフィックを許可するために1以上のACLを生成する過程とを特徴とする方法。

【請求項10】 前記1以上のACLが異なるグループにおけるサブネットワーク間のトラフィックを検査する前記複数のグループを規定する過程を含むことを特徴とする請求項9に記載の方法。

【請求項 1 1】 1以上の其用サブネットワークの識別子を愛信する前記コンピュータシステムを更に含む前記方法において、トライフィックが、前記グループの何れか1つにおける各其用ネットワークと任意の別のサブネットワークの間において許可されし。

1以上のACLによつて、トライフィックが、前記グループの何れか1つにおいて前記其用サブネットワークの何れか1つとする請求項1の記載のサブネットワークの許可されることを特徴とする請求項1を特徴とする請求項1。

【請求項 1 2】 少なくとも1つの前記ドメインが、前記ドメインにおけるトライフィックを制限することが可能である請求項1の記載の方法において、前記コンピュータシステムが、前記グループにおいて許可及び／又は拒否されたトライフィックを識別するための情報を愛信する過程であつて、前記情報を、制限するトライフィックにおける1以上のドメインによる指連に従つてトライフィックを許可及び／又は拒否するように、前記コンピュータシステムがトライフィックを制限可能なドメインを構成する過程とを更に含むことを特徴とする請求項1に記載の方法。

【請求項 1 3】 所定のグループ内において許可及び／又は拒否されたトライフィックを識別するための情報が、1以上の（1）トライフィックを制限可能なドメイン内のトライフィックを各々送信する1以上のスイッチのポートであつて、前記グループ内のトライフィックを運ぶための前記ポートと、（2）前記グループに属するエンティティの物理的なアドレスと、更に（3）前記グループ内のトライフィックの送信又は愛信を許可されたユーザ名との識別子を含むことを特徴とする請求項1 2に記載の方法。

【請求項 1 4】 各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項1に記載の方法。

【請求項 1 5】 前記1以上の装置が、IPアドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トライフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項1に記載の方法。

【請求項 1 6】 ネットワークドメインのトライフィックの経路を指定す

る以上の複数に対して以上のアクセス制御リスト (ACLs) を生成するための所定の構造体において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間ににおいてどのようなトライックが許可及び／又は拒否されるかを決定し、更に、

各グループ内においてトライックが許可されるよう、サブネットワークの以上のグループをコソビュータシステムに対して規定する手段であつて、各サブネットワークがネットワークドメインの一部であるか、或いはネットワークドメインの全てであり、また各グループに対して、前記グループに属するサブネットワークの識別子をコソビュータシステムによって説明するための前記規定手段と

前記コソビュータシステムによって、各グループ内のトライックを許可するための以上のACLを生成するための手段とを含むことを特徴とする構造体。

【請求項17】 前記構造体が、前記コソビュータシステム及び該コソビュータシステムにロードされた所定のプログラムを含み、前記コソビュータシステムと前記プログラムとの組合せが、前記規定手段及び生成手段を含むことを特徴とする請求項16に記載の構造体。

【請求項18】 前記構造体が、前記規定手段及び前記生成手段を実施するための命令を含むコソビュータの説明り可能構体であることを特徴とする請求項16に記載の構造体。

【請求項19】 前記規定手段が複数のグループを規定するときに、前記1以上のACLが異なるグループににおけるサブネットワーク間のトライックを拒否することを特徴とする請求項16に記載の構造体。

【請求項20】 1以上上の共用サブネットワークの識別子を前記コソビュータシステムによって説明するための手段を更に含む前記構造体において、前記グループの何れか1つにおける各共用サブネットワークと他の任意のサブネットワークとの間でトライックが許可され、1以上の前記ACLによって、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任意のサブネットワークとの間でトライックが許可されることを特徴とする請求項16に記載の構造体。

【請求項 2.1】 少なくとも 1 つの前記ドメインが、前記ドメインにおけるトライックを制限可能であるよるような前記構造体であつて、前記グループの各々に対しても、前記グループ内に表示する許可及び／又は拒否されたトライックを識別するための情報を前記コンピュータシステムによつて読み取るための手段であつて、前記情報が、前記情報において 1 以上のドメインによつて復用されるような読み取り手段と、

前記情報による指定に従つてトライックを許可及び／又は拒否するよるに、トライックを制限可能な各ドメインを前記コンピュータシステムによつて構成するための手段とを更に含むことを特徴とする請求項 1.6 に記載の構造体。

【請求項 2.2】 所定のグループ内において許可及び／又は拒否されたトライックを識別するための情報が、1 以上 (1) トライックを制限可能なドメイン内のトライックを各々送信する 1 以上のスイッチのポートであつて、前記グループ内のトライックを運ぶための前記 1 以上のポートと、(2) 前記グループに属するエンティティの物理的アドレスと、更に (3) 前記グループのトライックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項 2.1 に記載の構造体。

【請求項 2.3】 各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項 1.6 に記載の構造体。

【請求項 2.4】 前記 1 以上の送信が、即アドレスに基づきトライックの経路を指定し、また各ドメイン内において、トライックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項 1.6 に記載の構造体。

【請求項 2.5】 複数のドメインのネットワークにおける接続を確立するための方法において、少なくとも 1 つのドメインが、前記ドメインにおいて規定されたサブドメインを有することをができ、前記ドメインのトライックが拒否され、更に、各グループ内においてトライックが許可されるようない以上の接続グループを規定する過程であつて、少なくとも 1 つの接続グループに対して、コマンダシステムに前記接続グループに属するトライックを規定する情報を与えるよ

うな前記規定過程と、

少なくとも1つの接続グルーブに対して、前記コンピュータシステムに前記接続グルーブのメンバであるサブドメインの識別子を每える過程と、
少なくとも1つの接続グルーブに対して、前記サブドメインに付て前記接続グルーブにおけるトライックが許可されるように、前記コンピュータシステムが、前記接続グルーブにおけるサブドメインを有する各ドメインを構成する過程とを含むことを特徴とする方法。

【請求項26】 トライックを規定する前記情報が、少なくとも1つのグルーブに対して、以上に(1)单一のドメイン内のトライックを各々送信する以上のスイッチのポートであって、前記ダブループ内のトライックを運ぶための以上の前記ポートと、(2)前記ダブループのメンバである端末の物理的アドレスと、更に(3)前記ダブループ内のトライックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項25に記載の方法。

【請求項27】 各々のドメインを構成する過程が、前記ダブループにおけるサブドメインを有する单一のドメイン内のトライックを送信するスイッチについて、(a)前記ダブループのメンバである端末の物理的アドレス間のトライックを許可するための、また(b)異なるダブループのメンバである端末の物理的アドレス間のトライックを拒否するための前記スイッチが許可される過程を含むことを特徴とする請求項26に記載の方法。

【請求項28】 複数のドメインを含む所定のネットワークにおける接続を確立するための構造において、少なくとも1つのドメインが、前記ドメインにおいて規定されたサブドメインを有することが可能であり、前記ドメインによって、单一のサブドメイン内のトライックが許可されるが、サブドメインのトライックが拒否され、更に、以上の接続ダブループにおける各接続ダブループに属するトライックを規定する情報をコンピュータシステムによつて送信するための手段であつて、トライックが各ダブループ内で許可されるような前記受信手段と、少なくとも1つの接続ダブループについて、前記接続ダブループのメンバであるサブドメインの識別子を前記コンピュータシステムによつて送信する手段と、

少なくとも1つの接続グループについて、前記サブシステムによつて前記接続グループにおけるトライックが許可されるよう、前記接続グループにおいてサブドメインを有する各ドメインを前記コントローラシステムによつて構成するための手段とを含むことを特徴とする所定の構造体。

【請求項29】 トライックを規定する前記情報が、少なくとも1つのグループに対して、1以上の(1)單一のドメイン内のトライックを各々送信する以上のスイッチのポートであつて、前記グループ内のトライックを選ぶための1以上の前記ポートと、(2)前記グループのメンバである端末の物理的アドレスと、更に(3)前記グループ内のトライックの送信又は受信を許可されたユーザ名との識別手順を含むことを特徴とする請求項28に記載の構造体。

【請求項30】 前記構造体が、前記コントローラシステム及び該コントローラシステムにロードされた所定のプログラムを含み、前記コントローラシステムと前記プログラムとの組合せが、前記全ての手段を含むことを特徴とする請求項28に記載の構造体。

【請求項31】 前記全ての手段を実施するための命令を含むコマンダの読み取り可能な媒体であることを特徴とする請求項28に記載の構造体。

【請求項32】 各ドメイン内のトライックが、端末の物理的アドレスに署づき端末間で送信され、またドメイン間のトライックが、端末の論理的アドレスに基づき経路指定されることを特徴とする請求項28に記載の構造体。

【発明の詳細】

【0001】

発明の概要

本発明はネットワークに属するもので、また詳細にはネットワークにおける接続性の確立に係るものである。

【0002】

セキュリティ上の理由やネットワークの通信量を低減する目的で、幾つかのネットワークでは接続を制限している。従って、ネットワークにおける幾つかの端末が互いに通信を許可される一方で、別の端末または通信を許可されない。後続では、通信を許可された端末間の物理的な通信リンクが確立されることによって性能となるが、既には通信を許可されていない端末間の物理的な通信リンクが確立されないことをによって禁止される。しかし、これは各セットの接続の制限のための物理的リンクを個別に構成することが必要であるので実際的ではない。従つて、コマンドを発行してネットワーク接続を割当ることによってネットワークの接続性を確立する或いは変更するための技術が発達してきた。

【0003】

これについて図1及び図2に示す（これらの図には先行技術にはない、本発明の幾つかの特徴が示してある）。ネットワーク110は、大規模な組織の相互接続に適する企業ネットワークである。ネットワーク110には、第2層ドメイン（layer 2 domains）116P、116Q、116R、116S、116Tが含まれる（用語「第2層」は、D. Biererらの”NetWare⁴ for Professionals”（1993）、1-9頁、ここで省略する）とにより本明細書の一部とする）に記載のOSI参照モデルを指す）。同一の第2層ドメイン116に属する端末124（例えば、ドメイン116Pにおける端末124、1、124、2）は、それらのMACアドレス（「第2層」アドレス）を用いて互いに通信可能である。MAC（媒体アクセス制御）アドレスは、端末のネットワークインターフェースカード（NIC）に書き込まれた物理的アドレスであるか、又はNICスイッチの設定によって確定された物理的アドレスである。全てのドメイン116又はその幾つかには、以上のネットワークスイッチ（NICスイッチ）と混同しないことが得られる。各ドメイン116のスイッチ128は

、端末のMACアドレスを用いて端末1、2、4間でトライックを送信する。

【0004】

異なる第2層ドメインにおける端末（例えば、端末124.1、124.3）は、MACアドレスのみを使用して互いに通信することができない。それらは、論理アドレスであるIPアドレスを用いて通信する。ルータ130.1、130.2、130.3は、端末のIPアドレス（必要に応じてIPアドレスとMACアドレスとの間で変換される）に基づきドメイン116間のトライックの経路を指定する。

【0005】

幾つかのドメイン116においては、ペーチャルLAN（単一、VLAN）を用いて接続性を制限することができます。例えば、ドメイン116Pには3つのVLAN 140a、140b、140cが含まれる（図2）。ドメイン116Pにおける端末124は、それらが同一のVLANに属している場合にのみ、第2層において（即ち、それらの第2層アドレスを用いて）互いに通信可能である。従って、図1に示すVLAN 140aに属する端末124.1、124.2は通信可能である。

【0006】

VLANは、LANスイッチ128によって実現される。詳述すると、スイッチ128は、同一のVLAN内の端末間のみでパケットを送信する。（スイッチ128は、VLANへのトライックを制限可能なので、「VLAN-capable」と称される。例えば、ドメイン116S、116Tのような幾つかの第2層ドメインには、「VLAN-capableスイッチが含まれる。）

異なる第2層ドメイン間の接続が本、ルータ130によつて制限される。ルータ130は、IPアドレスに基づき接続の制限を規定するアクセス制御リスト（ACLs）を使用する（例えば、K. Siyan及びC. Bareの“Internet Firewalls and Network Security”（1995）、187-192頁を参照）。

【0007】

アクセス制御リストの作成及びVLANの規定は、ネットワーク管理者を混乱させた面倒なプロセスであり得る。このプロセスは、動的ネットワーク環境においては度々繰返されねばならず、そこでは端末、ユーザ、及びネットワークサービスが異なる場所から別の場所へ移動し、又は物理的な移動なしに或る組織から他の組織へ

織へ移され、或いは付加もしくは除去される。

【0008】

従つて、ネットワークにおける接続の設定を容易にすることが望ましい。

【0009】

発明の開示

本発明は、ネットワークの接続を確立及て制御するための新しい方法をシステムを提供するものである。幾つかの実施例においては、VLAN及びアクセス制御リストの容易な生成が可能となる。

【0010】

幾つかの実施例においては、アクセス制御リストが管理端末(management station)によって作成される。管理端末は接続グループの規定を受信する。各接続グループ(connectivity groups)はサブネットワークのグループである。トライフィックは各グループの中で許可される。幾つかの実施例において、各サブネットワークはIPサブネットとして識別される。管理端末は、接続グループを規定する情報からアクセス制御リストを作成する。

【0011】

幾つかの実施例において、管理端末は其用サブネットワークの識別番号を変換し、また任意の接続グループにおける任意のサブネットワークと共用サブネットワークとの間のトライフィックを許可するACLを作成する。

【0012】

幾つかの実施例において、管理端末は、例えばVLANのようなサブドメインを、ドメインを適切に構成することによって生成する。ネットワーク管理者は、ドメインを構成するためにそのグループに属するトライフィックを規定する各接続グループ情報に入力する。そのような情報の例には、同一の接続グループに属するエンティティ(例えば、スイッチのポート、ネットワーク端末のMACアドレス、又はロジオシティからのエンティティは通信を許可されるユーザ名)のリストが含まれる。異なる接続グループによって指定されるユーザ名のリストが含まれない。接続グループは、異なる第2層にメインからのエンティティを含み得る。エンティティは、どのエンティティがどのVLANに属するかを指定することなしに、接続グループに対して割

当てられる。管理端末は、同一のグループにおける何れのエンティティが所定の群のドメインに属するかを決定し、そのようなエンティティを適切なVLANに配信する。

【0013】

幾つかの実施例において、接続グループにおけるトラフィックを規定する情報には、第2層パケットのビットの値が含まれる。

【0014】

本発明は、第2層ドメイン、スイッチ、又はルータに限られるものではない。本発明の他の特徴及び優位性については後述する。本発明は添付した請求の範囲で規定されるものである。

【0015】

発明の詳細本説明

ネットワーク1.10には、5つの第2層ドメイン1.6が含まれる。各ドメインにおけるパケットのアドレス指定が、OSI参照モデルの第2層（データリンク層）におけるパケットの内容に基づき行われるので、これらのドメインは「第2層」と称される。ルータ1.30は、第3層（ネットワーク層）におけるパケットの内容に基づきトラフィックの経路を指定する。特に、IPアドレスは、第3層のアドレスである。しかし、本発明は第2層若しくはOSI参照モデルに従うネットワークに限定されるものではない。

【0016】

ドメイン1.16Pには、MACアドレスに基づきトラフィックを送信するVLAN-capableスイッチ128.1、128.2が含まれる。それらのスイッチは、トランク150.1によって互いに接続されている。各スイッチは、ネットワークセグメントに各々接続されている以上のポートを有する。従って、スイッチ128.1のポート160.1は、端末124.1を含むネットワークセグメントに接続されている。また、スイッチ128.2のポート160.2は、端末124.2を含むネットワークセグメントに接続されている。図1において、各ネットワークセグメントは單一の端末を含む。成る実施例においては、ネットワークセグメントは複数の端末を含む。

【0017】

スイッチ128.1のポート160は、後述するような接続マップの生成に用いられる端端端末124Mに接続される。

【0018】

スイッチ128.1は、トランク150.2によつてルータ130.1に接続される。ルータ130.1は、ルータ130.2、130.3、及びインターネット170に接続される。ルータ130.2は、ルータ130.3に接続される。ルータ130.2は、トランク150.3によつてドメイン116QのVLAN-capableスイッチ128.3に接続される。ドメイン116Qには、VLAN-capableスイッチ128.4、128.5、及び128.6が含まれ、その名はスイッチ128.1、128.2と同様に1以上の中ネットワーカセグメントに接続される。ここでは、端末124.3を含むセグメントのみ示す。また、ドメイン116Qのスイッチ128は互いに接続されている。

【0019】

ルータ130.2は、第2層ドメイン116Tに接続されている。

【0020】

ルータ130.3は、ドメイン116RのVLAN-capableスイッチ128.7及び第2層ドメイン116Sに接続されている。スイッチ128.7は、スイッチ128.1、128.2と同様にネットワーカセグメント(図示せず)に接続されている。ドメイン116S、116Tはスイッチを全く含まないか、或いは幾つかのスイッチ(図示せず)を含む。

【0021】

幾つかの実施例において、1以上のドメイン116はスイッチを全く含まないか、或いは非VLAN-capableスイッチ、ハブ又はコンセントルータ含む。

【0022】

前述のように、異なるドメイン間の通信にはIPアドレスが使用される。例えば、端末124.3にパケットを送信するたまに、端末124.1は、端末124.3のIPアドレス及びMACアドレスを、それを元の物理的先アドレス及び物理的後アドレスとしてパケットに書き込む。ルータ130.1は、祖先MACアドレスをルータ130.2のMACアドレスと書き換え、端末124.1の発信元MACアドレスをルータ130.1のMACアドレスに書き換える。次にルータ130.1が、パケットをルータ130.2に送

信する。ルータ130.2トは、ノードセットの発信元をMACアドレスを自身のMACアドレスに纏き纏え、来た宛先MACアドレスを端末124.3のMACアドレスに纏き換えて、ノードセットをスイッチ128.3に送信する。スイッチ128.3は、ノードセットをスイッチ128.5経由で端末124.3に送信する。ドメイン1116Pには複数してないVLAN140a、140b、140c、140d、140e、140fが含まれ、ドメイン116Qには、重複してないVLAN140g、140h、140iが含まれ、ドメイン116Rには重複してないVLAN140j、140k、140lが含まれる。VLANにおける各端末のメンバーシップは、端末が接続されているスイッチポート160によって規定されるか、端末のMACアドレスによって規定されるか、既に端末にログオンしたユーザーのユーザ名によって規定される。ポート又はMACアドレスに基づくVLANのメンバーシップの確定については、6. Heldの“Virtual LANs: Construction, Implementation, and Management”(1997), 233-249頁(ここで著者すむことにより本明細書の一部とする)に開示されている。

【0023】

ユーザー名によるVLANのメンバーシップの確定については、付録Aに記載されている (“User-Based Binding of Network Stations to Broadcast Domains” と題する)、Ekströmらの米国特許出願08/832,011(1997年4月2日出願; ここで普及することにより本明細書の一部とする)を参照)。或る実施例においては、VLAN140が、ポートによって識別される端末、MACアドレスによつて識別される端末、及びノード名によつて識別される端末を組び合わせる。

【0024】

ドメイン116S、116Tは、任意のVLANを含む場合もあり、また含まない場合もある。

【0025】

管理端末124Mは、VLAN140hに属する。端末124Mは、任意のスイッチ128及び任意のルータ130と通信可能である。既る実施例において、(1)全てのスイッチ128は、Cisco社(San Jose, California)から入手可能なもの、(2)ルータ130は、Cisco社から入手可能なルータであり、それらはCisco社の説明書に記載されている(説明書等)

8-2040-01）。これらは、ここで書及することにより本明細書の一部とする。

【0026】

ネットワーク 110 には、種々のドメイン 116 におけるエンティティ（非トランクスイッチポート 160、MAC アドレッサー、又はユーザ名）を含む接続グループが含まれる。例えば、接続グループは、VLAN 140 a、140 d、140 g における全てのエンティティによって構成され得る。通信は、同一の接続グループにおいては直接行われ、異なる接続グループにおけるエンティティ間においては経路選擇される。詳述すると、スイッチ 128 及びルータ 130 は、異なる接続グループにおける端末 124 から別の接続グループにおける端末 124 へのパケットの経路は指定しない。

【0027】

周知のように、VLAN は第 2 層通信ドメインである（また、ここでは「第 2 層間報通信ドメイン」又は「第 2 層 BD」と称される）。対照的に、接続グループは必ずしも間報通信ドメインではない。従って、幾つかの実施例においては、間報通信又はマルチキャストトラフィックは單一の VLAN に制限される。

【0028】

また、本明細書において VLAN は「ノード間報通信ドメイン」即ち VBD と称される。VBD は、ネットワークに於いて必ずしも物理的な接続（例えば、ケーブル）の変更の必要なしに規定され得る間報通信ドメインである。

【0029】

管理端末 124 M には、プログラムやデータを記憶するための記憶装置 192 0 及びデータアクセス制御リストを生成する）プロセスを示している。ここで、このプロセスは図 1 の VLAN の例に示しており、また 3 つの接続グループは以下の通りである。

【0030】

付録 B は、幾つかの実施例における接続グループを生成する（特に、VLAN 140 及びルータアクセス制御リストを生成する）プロセスを示している。ここで、このプロセスは図 1 の VLAN の例に示しており、また 3 つの接続グループは以下の通りである。

【0031】

グループ1は、VLAN140a、140d、及び140gからなる。

【0032】

グループ2は、VLAN140b、140e、及び140hからなる。
このグループは、管理端末124Mを含む管理接続グループとして指定され得る。)

グループ3は、VLAN140c、140f、及び140iからなる。

【0033】

幾つかの実施例においては、第2層にメイン116Sは間報通信ドメインである。付録Bのプロセスは、ドメイン116Sを、任意の接続グループとの連絡を許可された共用IPサブネットとして構成する。重要なことは、各第2層間報通信ドメインが、IPサブネット又はIPサブネットの組合せであることである。

【0034】

付録Bのプロセスは、第2層ドメイン116T及び間連するサブネットを「非管理(unmanaged)」状態にする(即ち、対応するルーチンタスクエースに対してACLが生成されず、更にプロセスによつて生成された任意のACLにおいてサブネット116Tは表示されない。)。従つて、ドメイン116Tは任意の接続グループからトラフィックを受取り可能であるが、ドメイン116Tから任意の接続グループへのトラフィックは、ルータ130によつて取除かれ得る(遮断され得る)。

【0035】

幾つかの実施例において、單一の第2層ドメインには、管理されたサブネット及び非管理のサブネットが含まれる。

【0036】

付録Bのプロセスは、任意のVLAN又は接続グループがネットワーク110において確立される前が既には確立された後に実施され得る。幾つかの実施例において、付録Bプロセスが最初に実施され、全てのドメイン116(場合によつて、ドメイン116S、116Tのような共用ドメイン及び非管理のドメインのエンティティを除く)における全ての通信エンティティを含む單一の「管理接続グループ(management connectivity group)」を確立する。その管理グループによつ

て、管理端末124Mが全てのスイッチ及びルータと通信可能となる。次に付録Bプロセス又は付録Gのメントナンバングループ1、2、3又は別の任意のグルーブを確立する。そのようなグルーブの設置は、管理端末がスイッチ及びルータと通信する能力によって容易となる。

【0037】

戴いは、管理端末124M及びスイッチ128のルートのみが管理接続グルーブに配置され。幾つかの実施例においては、スイッチ128のそれらのポートのみが管理接続グルーブに配置され、その管理接続グルーブは管理端末124Mを全てのVLAN-capableスイッチ及び全てのルータと通信可能とするなどを要求される。

【0038】

後述する実施例においては、付録Bプロセスの開始段階に接続グルーブが存在しないと假定する。

【0039】

付録Bのプロセスが開始される前に、各ルータ130が構成されて、1以上のIPサブネットが各ルータ210に割り当てられる(図2)。Cisco社の説明書において「サブインターフェース」と称される幾つかに対して、ここでは用語「インターフェース」を用いることに注意されたい。)付録Bのプロセスが完了した後に、各ルータ130は、それらが接続されるドメイン116の各VLAN140に対して個別のサブネットを有し得る。

【0040】

各VLAN140はサブネット又はサブネットの組合せであるので、経路指定ソフトウェアがVLANを明確に認識しない場合でも、ルータ130がVLANに基づき事实上の送信決定を行なうことには注意されたい。ルータは、ルータのトランクポート(例えば、トランクポート220)経由でメインに接続され、また各インターフェースはトランクポートの論理的サブポートである。

【0041】

周知の通り、ルータ及びスイッチのトランクポート(即ち、スイッチ、又はスイッチ及びルータと相互接続するトランク150に接続されたポート)は、マル

チフルVLANのためのトラフィックを運ぶ。トランクポートにおけるトラフィック
はトランクプロトコル(trunking protocol)を使用し、そこで各マケットは、パ
ケットが割当てられるVLANの識別子を標識したより大きなパケットに内包化
(encapsulated)される。VLANエンベーシングするMACアドレスよりも繋るポートに
よって規定される場合、VLANの標識にまつて愛憎スイッチ128がシケシトのV
ANを識別することができる。

【0042】

ルーター130はトランクポートを理解し、同一のトランクポートにおける
種々のVLANからのトラフィックを、各VLANからのトランクがVLANを割当てら
れた個別のポートに到達した場合のように取り扱う。

【0043】

幾つかの実施例においては、トランクの代わりにルータと第2層ドメインとの
間の個別の物理的接続を用いて個々のVLANに対するトラフィックを運ぶ。

【0044】

各インターフェースは、インターフェースによって取扱われるサブネットにおける
ゲートウェイアドレスを有する。ゲートウェイアドレスは、サブネットにおける
ルータのアドレスである。

【0045】

付録Cは、記憶装置192において付録Bの幾つかのステップによつて作成さ
れたデータベースを示す。

【0046】

ステップM5(付録B)において、ネットワーク管理者は、管理端末124M
にネットワーク1.1.0のIPアドレスを等える。付録Bの例において、アド
レスレンジは10.0.0.0/8である。ネットワーク1.1.0において、各サブネットは
255.255.255.0のサブネットマスクを有する。

【0047】

IPアドレスレンジ及びサブネットは、形式10.0.0.0/8(サブネットマスクは、
全て0が繰く有り8つの1を有する)を有するか、或いはIPアドレス(10.0.0.0
)及びネットマスク(255.0.0.0)の組合せののような形式を有する。

【0048】

付録CのI.1に示すように、管理端末124Mはネットワーク110のDIPアドレスレンジをそのデータベースに入力する。

【0049】

付録Bに示すように、ステップM4が管理者によって実施される。端末124Mがデータ構造I.2を生成する(付録C)。この情報及び手録Cにおける他の情報は、異なる実施例においては異なって編成される。例えば、幾つかの実施例において、項目I.2-1(スイッチのアドレス)は、各ドメインに対するアドレスリストとして格納される。別の実施例においては、同様の情報は、アドレス及び各ドメインのペアとして格納される。別の実施例においては、他のデータ構造が用いられる。

【0050】

ステップM10において、ネットワーク管理者がVLAN140を規定する。VLANの規定には、各ドメインI.1.6における各スイッチI.2.8及び端末I.2.4Mに対してVLAN識別子を毎える過程が含まれる。VLAN識別子は、スイッチI.2.8に認識可能な識別子(即ち、VLAN番号)である。例えば、スイッチI.28.1、I.28.2の各々は、VLAN140a、I.40b、I.40cの識別子を愛憎し、スイッチI.28.7は、VLAN140g、I.40b、I.40iの識別子を愛憎する。VLANを規定する過程には、何れのエンティティ(ポート、MACアドレス又はエーチ名)が各々のVLANに属するかを明らかにする過程は含まれない。

【0051】

或る実施例においては、管理者がVLAN識別子を各スイッチI.2.8に直接入力する。別の実施例においては、管理者がVLAN識別子を各ドメインI.1.6の制御スイッチI.2.8に入力する。制御スイッチは、同一のドメインにおける別のスイッチ(假に存在すれば)に対して識別子を送信する。更に別の実施例においては、管理者はこの情報を例えばSNMP又はTelnet又はDIPプロトコルを用いて端末I.2.4Mから遠隔のスイッチI.2.8に情報を与える。

【0052】

付録CのI.3に示すように、端末124Mはこの情報をそのデータベースに格

納する。

【0053】

ステップM1.4において、ネットワーク管理者は情報1.4（付録C）を端末12.4Mに入力する。図1及び図2において、個々のサブネットトは各第2層BDに割当られ、第2層BDとIPサブネットとの間に1対1対応が存在する。サブネットは、図2及び次の表1に示されている。

【0054】

【表1】

表1

第2層BD	サブネット
140a	10.1.1.0/24
140b	10.1.2.0/24
140c	10.1.3.0/24
140d	10.2.1.0/24
140e	10.2.2.0/24
140f	10.2.3.0/24
140g	10.3.1.0/24
140h	10.3.2.0/24
140i	10.3.3.0/24
116s	10.3.4.0/24
116t	10.2.4.0/24

【0055】

幾つかの実施例においては、複数のサブネットが第2層BDに付して割当てられている。

【0056】

サブネットトは、サブネットマスクの表記法、又はサブネットアドレス及びマスクの表記法における1つのサブネットアドレス／番号を用いて端末12.4Mに与えられる。

【0057】

またステップM14において、対応するIPサブネットからの各VLANにおけるIPアドレスを割当るためにネットワーク110が構築される。従つて、幾つかのWindows NT[®]の実施例において、DHCPサーバーは各サブネットににおいてIPアドレスを割当するために構成される。(Windows NTにおいては、例えば、Sant' Angeloらの“Windows NT Server Survival Guide”(1996)に記載されており、これについても、ここで言及することにより本明細書の一部とする。)幾つかの実施例においては、DHCPサーバがルート130においてサブネットの1つに接続される。ルータは、DHCPのリクエストをルータに直送するように構成される。別の実施例においては、側面のDHCPサーバへ送信するように構成される。別の実施例においては、側面のDHCPサーバが各サブネットに設けられる。

【0058】

ステップM20において、各接続グルーブに対して、管理者は接続グルーブのメンバであるIPサブネット(即ち、接続グルーブのメンバである第2層BDの一部であるIPサブネット)を端末124Mに入力する。従つて、管理者は、接続グルーブに対してVLAN140a、140d、140gににおけるサブネットを入力し、グルーブに対してVLAN140b、140e、140hにおけるサブネットを入力し、更にグルーブに対してVLAN140c、140f、140iにおけるサブネットを入力する。或いは、各接続グルーブに対して、管理者は、接続グルーブの第2層BDメンバの識別子を入力する。各々のケースにおいて、全てのルータを管理端末124Mから到達可能とすると、管理者は、接続グルーブのメンバであるIPサブネットを入力し得る。幾つかの実施例において、各ルータは、共有サブネット又は管理接続グルーブのサブネットメンバにおける少なくとも一つのゲートウェイIPアドレスを有する。

【0059】

幾つかの実施例では、全てのルータが管理端末から到達可能であることを必要としない。従つて、管理者されていないサブネット及び他のルータにのみ直接接続されたルータは、幾つかの実施例においては到達可能であることを必要としない。

【0060】

項目I 5 (付録C) が、ステップM 20において生成される。

【0061】

多數のサブネットが単一の第2層 BDに割当された場合、それらは全て同じ接続グループに割当られる。

【0062】

ステップM 30において、管理者が各接続グループに属するエンティティを端末124Mに入力する。ここで、I 6 (付録C) が生成される。例えば、接続グループ1の場合、管理者はスイッチポート160.1、160.2、160.3 (ポート160.3に接続された端末124.3はVLAN 140dに属すると仮定する)、及び他のポート、MACアドレス、並びに／又はVLAN 140a、140d、140gに属するユーザ名を入力する。幾つかの実施例においては、管理者は、ポート、MACアドレス又はユーザ名がどのドメイン又はVLANに属するかを記憶する必要がない。

【0063】

ポート160は、参照が容易なように管理者によつて割付けられるラベルによつて、端末124Mにおいて識別される。例えば、ポートがユーザ名Fredのユーザによって使用される端末124に接続されている場合、管理者はそのポートにラベル「Fred」を割付けができる、またステップM 30において「Fred」を入力してこのポートを接続グループに割付けることが可能である。MACアドレスの接続グループへの割付けも同様である。

【0064】

ステップM 40において、管理者は情報17A及び18 (付録C) を管理端末124Mに入力する。

【0065】

ステップM 45において、端末124MがVLAN 140を生成し、付録Dに示すように各エンティティを適当なVLANに配置する。付録Dにおいて、括弧内の番号は、付録Dの対応するステップにおいて用いられる付録Cのデータベース項目を指す。

【0066】

半端Dにおいて、接続グループのエンティティEがVLAN…capableスイッチ（ステップV1）のポート160である場合、そのエンティティEはポートが属するドメイン116のVLANにのみ配置される。対照的に、エンティティEがMACアドレステップV2）又はユーチャ（ステップV3）である場合、そのエンティティEは接続グループの全てのVLANに配置される。MACアドレスの場合では、これによりてMACアドレスを有する端末が、その接続グループのVLANを含む任意のドメイン116に接続され得る。従って、接続グループにおけるMACアドレスを有する携帯用コンピュータ（例えば、ラップトップコンピュータ）は、ドメイン116P、116Q、116Rに接続され得る。コンピュータがドメイン116Pに接続される場合、送信元アドレスとしてコンピュータのMACアドレスを有するパケットを送信するスイッチ128.1、128.2によって、コンピュータがVLAN140aに配置され得る。同様に、例えばコンピュータがドメイン116Qに接続される場合、それはVLAN140dに配置され得る。

【0067】

同様に、ユーチャ名が接続グループの全てのVLAN140に配置される。ユーチャがドメイン116Pにログオンした場合、ユーチャを適切なVLANに切替えるためにUBNCサーバーへに対する要求がドメイン116Pから届く。例えばユーチャ名が接続グループ1に存在する場合、UBNCサーバーはユーチャをVLAN140aに配置する。同様に、ユーチャがドメイン116Q又は116Rにログオンする場合、UBNCサーバーは、ユーチャをVLAN140d又は140gにそれぞれ配置する。

【0068】

ステップV3において、「実施例1」は接続グループに関する任意の事項を知るためにUBNCサーバーを必要としない。端末124Mは、各ドメイン116におけるユーチャ名に対応してどのVLANが割当てられるかをUBNCサーバーに知らせる（ステップV3-2）。実施例2においては、UBNCサーバーはどのVLANがどの接続グループに属するかを認識している（この情報はUBNCサーバーへに直接与えられるか、或いは例えば端末124Mから遠隔的に与えられる）。従って、実施例2のステップV3-1において、端末124MはどのVLANがユーチャがログオンが生じたサーバーへに通知しない。ユーチャがログオンした時、UBNCサーバーはログオンが生じた

ドメイン 116 及びユーザの接続グルーピングからエーテル VLAN を決定する。UBNC データベースには、各ドメイン 116 における各 VLAN における IP サブネットが含まれるので、ドメイン 116 はユーザの IP アドレスから決定される。幾つかの実施例においては、UBNC ネットワークは管理端末 124M において作動する。

【0069】

ステップ M50 (付録 B)において、端末 124M は、付録 E におけるプロトコルを実行することによって、ルータアクセサリスルーパのサブネット番号が直接接続及び付録 A 1 のアクセサリスルーパに対する作成される。付録 E のプログラムは、ルータ 130, 2 から VLAN 140 までのインターフェース 210 の例において説明される。

【0070】

各ルータインターフェースに対して、対応するサブネットが所定の接続グルーピングに属する場合、付録 F によつて、ルータアクセサリスルーパ A1 から A5 によつてアクセサリスルーパのサブネット番号 (例えば、A1—1) は、付録 E のステップ番号に付録 A1 (付録 E) は回線 A1—2a 及び A1—2b を生成する。

【0071】

付録 F は、CiscoNet (San Jose, California) の幾つかのルータによつて用いられるシナリオを用いる。このシナリオについては、K. Siyan 及び C. Bare の "Internet Firewalls and Network Security" (1995), 186-191 頁に記載されており、これについてほほここで言及することにより本明細書の一部とする。回線番号 (例えば A1—1) は、アクセサリスルーパの一部ではない。更に、迷惑符 (!!) で始まり行の終わりまで続く文言は、ルータによつて無視されるコメントである。これらのコメントは幾つかの実施例においては省略される。

【0072】

ステップ A1 は、サブネット 116S のような各共用サブネットからのインターフェース 210 へのトライックを許すする。そのプログラムは、アクセリスト (access-list)、アクセス

制御リスト書録（幾つかの実施例においてプログラム自身によつて連続的に発生する）、「許可 ip (permit ip)」、実行サブネットのIPアドレス、並びに0.0.0.255のワイルドカードマスクを書き込む。（入力のパケットIPと比較して、ワイルドカードマスクにおける0比特は、發信元IPアドレスの対応するビットがワイルドカードマスクにおける1比特は、対応するビットが使用されていないことを示す。）

回線A L1-1におけるワイルドカードマスク0.0.0.255は、サブネットマスクを反転させることによって決定される。

【0073】

ステップA 2は、同一の接続グループにおける他の全てのサブネット（即ち、第2層 BD）からのトラフィックを許容する例えは回線A L1-2 a、A L1-2 bのような回線を生成する。回線A L1-2 aは、サブネット10.1.2.0/24 (VLAN 140 b) からのトラフィックを許容する。回線A L1-2 bは、サブネット10.3.2.0/24 (VLAN 140 h) からのトラフィックを許容する。

【0074】

ステップA 3は、ネットワーク110における他の全ての端末からのトラフィックを拒否する回線A L1-3を生成する。（複数なことは、ルータがノードケットを受取ったときに、ルータがアクセス制御リストの始めからノードケットの開始をテストすることである。ノードケットに適合する行が発見されたとき、アタセス制御リストの残りの部分は無視される。）ワイルドカードマスクは、ネットワーク110のIPアドレスレンジマスクを反映させることによって得られる。

【0075】

ステップA 4において、インターネット110からのトラフィックを含むネットワーク110の外線の仕様の回線の端末からのトラフィックを許容する回線A L1-4が生成される。

【0076】

幾つかの実施例において、管理者は、ステップM 5 0の前に接続グループにおける各サブネットに対して、インターネットからサブネットへのトラフィックが許可されるかどうかを管理端末124 Mに示す。トラフィックが拒否された場合

は、対応するインターフェースに対してステップA4が省略され、またステップA3がライナル1-3の代わりの「任職の拒否ip (deny ip any)」回線を生成する。

【0077】

付録Eに示すようにステップA5が実施される。

【0078】

ルータインターフェースが接続グループのBDメンバに接続されずに、其用意しく非管理サブネット（例えば160.0.0.0）又はインターネット1.1.0に接続される場合、ACLは生成されずにはサブネット群しくはインターネットは他の任職のサブネットからアクセス可能となる。

【0079】

幾つかの実施例においては、付録BのステップM4.0において、管理者は各其用サブネットに對してどのようなアクセスが与えられるかを指定し、付録Eのプロセスによつて、当該者に周知の方法を用いて適切なアクセス制御リストが作成される。例えば、其用サブネットがネットワーク1.1.0の中からのみアクセス可能となる場合、アクセス制御リストは以下のよう構成される。

【0080】

アクセスリスト1許可ip 10.0.0.0 0.255.255.255
アクセスリスト1拒否ip 任職

別の実施例において、そのような機能性は、ルータ130.1又は他の幾つかの機器（図示せず）において実現される企業全体に広がるファイアウォールによつて与えられる。

【0081】

管理者未124Mは、存在する全てのアクセス制御リストを消去して、新しいアクセス制御リストに置き換えるように各ルータ130に指示する。

【0082】

幾つかの実施例においては、ネットワーク管理者は追加のコマンドをアクセス制御リストに挿入する事が可能である。従つて、幾つかの実施例においては、管理者が、ステップM5.0の前に対応するインターフェースに対してアクセス制御

リストに挿入される各サブネットの追加項目を指定し得る。詳述すると、管理者はステップA1の前に挿入される項目、ステップA2とA3の間に挿入されると、管理者はステップA3とA4の間に挿入される項目、及びステップA4の後に挿入される項目を指定することができる。幾つかの実施例において、この技術を用いてファイアウォールの機能をアクセス制御リストに組込み、従つて、企業全体に渡る個別のファイアウォールの必要はなくなる。

【0.0.8.3】

幾つかの実施例においては、ステップM10及びM20が省略される。ステップM4～5において、各接続グループに対して、管理端末124Mは、VLAN—capableスイッチ及び接続グループにおける1以上のエンティティを有する各ドメイン116においてVLANを生成し、またVLANにエンティティを配置する。（従つて、ドメインが接続グループにおけるポート160を有する場合、或いは接続グループにMACアドレス又はユーザ名が含まれる場合に、VLANがドメインの中に生成される。）また端末124Mによって、IPサブネット（例えば、10.1.1.0/24）がVLANに割り当てられる。

【0.0.8.4】

幾つかの実施例においては、VLANのメンバーシップは、ポート、MACアドレス又はユーザ名以外の他の他の基準によって決定される。従つて、幾つかの実施例においては、VLANのメンバーシップは、例えば第2層パケットにおいての値のようなパケットの内容に基づき決定される。スイッチは28が、以上の値の求め決定されたセットの中にそのようなビットの値が存在するパケットを検取ると、そのスイッチは、パケットの発信元MACアドレス、又はパケットが到達するポート160を対応するVLANに配置する。スイッチ128がルータに接続されたトランクポートにおけるパケットを送信する場合、スイッチはパケットにVLAN番号はインタフェースが規定されたところに関連するものである。（この関係は、インターフェース210は、そのルータがに確立される。）従つて、図2に示すように、各ルータ130は、そのルータが直接接続される各サブネットに対する個別のインターフェース210を有する。特にステップM30に付録B～Cの実施例と同様に接続グループが生成される。

において、管理者は、各接続グループに対して、どのようなパケットがその接続グループに属するかを決定するルールを指定する。例えば、所定のルールによつて所定のビットの値を有するパケットが所属の接続グループに属するにとかが決定され得る。

【0085】

幾つかの実施例においては、ルータ130におけるアクセス制御リストによつて、IPアドレスとは別の基準に基づきトラフィックを許可するか或いは拒否する。例えば、ボート番号が関係する（例えば、W. Cheswick及びS. Bellovinの“Firewalls and Internet Security” (1994), 94-109頁を参照；ここで着及することにより本明細書の一部とする）。更に、所定の基準によつて、インターフェースへのトラフィックよりも寧ろインターフェースからトラフィックを指定する。管理者は、ステップMSOの前に端末124Mに対して十分な情報を与え、そのような基準に従つてアクセス制御リストを作成する。

【0086】

幾つかの実施例においては、冗長(redundancy)を目的として、VLAN140が間のルータの異なるインターフェース210に接続され得る。2つのインターフェースは、同一のサブネットか或いは2つの異なるサブネットに割当てられる。各ACLは、両方のインターフェースに対して同様の制限を与える。

【0087】

VLANが種々のルータのインターフェースに接続されるとき、場合によつては別のルータからアクセス可能な別の端末への接続の経路を指定するためには、ルータの1つがVLANを経由して別のルータへデータを送信することが可能である。その場合、VLANに接続されたインターフェースに対するACLが、ルータ間のトラフィックを適度に制限しないように構築される。幾つかの実施例においては、VLANサブネットは共同されるか或いは非管理であり、仕様の接続グループのメンバーではない。

【0088】

付録Gは、ネットワーク110において接続性を変更するためのメンテナンスプロセスを示す。付録Bのプロセスの再実行によつて、任意の変更を行うことが

可能である。しかしながら、幾つかの実施例において付録G プロセスがメンテナンスを容易にする。

【0089】

幾つかの実施例において、ステップM50は省略される (ACIは生じない)。

【0090】

前述の実施例は本発明を限定するものではない。本発明は、特定のネットワーク、層、スイッチ、ルータ、オペレーティングシステム、或いは他のハードウェア等はソフトウェアに限定されるものではない。また本発明は企業ネットワークに限定されるものではない。幾つかの実施例においては、MACアドレスはNICに書き込まれるものではなく、ソフトウェアによって生じる。幾つかの実施例において、付録B-6の管理ソフトウェアの全ては端末124より繋るスイッチ128又はルータ130で実行される。ソフトウェアは幾つかの実施例に適用される。

【0091】

幾つかの実施例においては、ドメイン116は第2層プロトコルとは別のプロトコルを使用し、ルータ130は、第3層プロトコルとは別プロトコルに基づきトラフィックの経路指定を行ふ。各ドメインにおける接続性は、MACアドレス又は第2層ペケットの内容とは別的情報に基づき決定され、ルータ130は、IPアドレスとは別的情報に基づきトラフィックを許容又は拒否する。幾つかの実施例においては、ルータ130はIPXアドレスを使用する。幾つかの実施例においては、D. Biererらの“NetWare 4 for Professionals”(1993) (ここで書及するにとにより本明細書の一部とする)に記載のネットワークアダプターのネットワークを復用する。他の実施例及び変更例は、添付した請求の範囲によつて規定される本発明の範囲内である。

付録△

ユーザベースネットワークユニットロール (UBNC)

幾つかの実施例において、VLANのメンバーシップは端末にログオンしたユーザに基づき決定される。Windows NTTM の幾つかの実施例においては、UBNCサーバが全てのVLANからアクセス可能なように設置される (例えば、サーバが其接サブネ

ツト内にある)。ネットワーク端末が能力アップされた(powered up)ときは、「デフォルト(default) VLANに配属される(デフォルトVLANは各々の第2層ドメイン116に存在する)。端末は、デフォルトVLANを提供するDHCPサーバーからIPアドレスを受取る。ユーザが端末にログオンした時、端末はUBNCサーバに対し、ログオン時に与えられたユーザ名に関連するVLANに端末を切替えるようにならざる。その要求には、ユーザ名、端末のMACアドレス、及び端末の現在のIPアドレスが含まれる。UBNCサーバは、UBNCサーバベースから関連するVLANを決定する。或る実施例においては、各ユーザ名に対して、データベースには関連するVLANの識別子が含まれる。別の実施例においては、データベースには管理端末によって与えられる以下のような情報が含まれる。

【0092】

- (A) 各ユーザ名について、そのユーザ名が属する接続グループの識別子
- (B) 各接続グループに属するVLANの識別子
- (C) 各VLANについて、関連するサブネット

UBNCサーバが要求を受取ると、サーバは要求する端末に対して(1)端末が属するVLANに切替えられるかどうかの指示(端末がデフォルトVLANにならないときにユーザがログオンした場合、切替が要求されない可能性があり、またVLANが規定されていないレイヤ2 BDにユーザがログオンした場合、切替が行われない可能性がある。)、並びに(2)ユーザがログオンしたVLANのIPサブネット及びサブネットマスクを送信する。次にUBNCサーバは、端末がそのDHCPリース(DHCP Lease)を解放するのを待つ。そこでUBNCサーバは、端末を含む第2層ドメイン116における单一のスイッチ又は複数のスイッチ128に対して適切なコマンドを送信する。そのスイッチによって、ユーティリティに割当てられたVLANに端末が配置される。

【0093】

UBNCサーバが端末の応答を受取った後に、端末はそのDHCPリースを解放し、次にサーバが端末を割当てられたVLANに切替え可能となるよう所定の期間待つ。その期間の後に、端末は切替が完了したと想定し、新たなDHCPリースの要求を送信する。応答において、端末は新たなIPアドレスを受取る。端末は新たなIPをUBNCサーバから受取ったサブネットマスク及びIPサブネットと照合する。新たなIPがサブ

ネットに存在しない場合、端末は新たな要素をUBMCサーバにに対して送出するごとに、よってその手続きを繰り返す。端末が新たなIPを要求したときに端末が割り当てられたVLANに切り替えられない場合、新たなIPは間違ったサブネットに存在する可能性がある。

【0094】

幾つかの実施例においては、サブオルトVLANは省略される。別の実施例においては、全ての端末又は地理的にもつとも近い端末のグルーブが個別のデバイスオルトVLANに割り当てられ、UBMCサーバによってエーザがそれらと関連するVLANに切り替わるまで通信を制限する。ユーザがログオフした時、ユーザ端末は適切なサブオルトVLANに戻される。

付録B

接続グループ(Connectivity Groups)の生成

M.5 管理端末 1 2 4 Mにネットワーク 1.1.0 の IPアドレスレジスト(例えば、10.0.0.8)を与える。

M.7 管理端末 1 2 4 Mに情報 I-2 (付録C) を与える。

M.10 VLANを定義する。

M.1.4 第2層 EDにIPサブネットを割り当てる。

M.2.0 各接続グループに対して、管理端末にグルーブのIPサブネットメッシュを与える。1つの接続グループを管理接続グループとして指定する。

M.3.0 後続グループに管理可能なエンティティ (ポート、MACアドレス及び／又はユーザ名) を割り当てる。

M.4.0 管理端末に情報 I-7 及び I-8 を与える

M.4.5 管理端末 1 2 4 Mが、エンティティを適切なVLANに割り当てる(付録D参照)。

M.5.0 管理端末 1 2 4 Mが、ルータのためのアクセス制御リストを作成する(付録E参照)。

付録C

管理端末データベース

I.1 ネットワーク 1.1.0 の IPアドレスレジスト

1.2 各ドメイン 16 における全てのVLAN—capableスイッチ 128

のIPアドレス

1.2-1 各スイッチのポートランクポート 16 の識別序
 1.3 各ドメイン 16 について、BDがVLANにおけるVLANの識別序
 1.4 各第2層 BDについて、BDがVLANであるか否か、またIPサブネットがBDに含まれているか否かの指示。BDがVLANである場合、VLANの識別序。

1.5 各接続グループについて、その接続グループに属するIPサブネット
 1.6 各接続グループについて、その接続グループに属するエンドティティ (ホスト、MACアドレス、及び／又はユーナメ)

1.7 各ルータインターフェースについて
 1.7-1 關連するサブネット (仮に存在すれば)
 1.7-2 インタフェースがVLAN—capable第2層ドメインに接続されているか否かを指示するフラグ

1.8 ネットワーク 110 における全ての共用サブネットのリスト

付録D

VLANの生成

各接続グループについて、また接続グループにおける各エンドティティ E (IG) について、

V.1 エンドティティ EがVLAN—capableスイッチ 128のポート 160 である場合、

V.1-1 ポートが属するドメイン 116-E (116P、116Q、116Rの一つ) を検索する (12-2、12-1)
 V.1-2 接続グループCC及びドメイン 116-E の両方に属するVLANを検索する (13、14、15)
 V.1-3 ドメイン 116-E のスイッチ 128 又はドメイン 116-E の御制スイッチ 128 に対してコマンドを送信することでポート E を VLAN に配置する

V.2 或いはエンドティティ EがMACアドレスである場合、接続グループCCにおける

各VLANについて(I4、I5)、

V2-1 VLANを含むドメイン116-V(I16T、I16Q、I16RのD1つ)を決定する(I3)

V2-2 ドメイン116-Vの制御スイッチ128又は全てのスイッチ128に対して適切なコマンドを送信することによってMACアドレスE5 VLANに割り当てる

V3 戦いはエンティティEがユーティリティCCに持ける各VLANについて(I4、I5)、

V3-1 VLAN(I3)を含むドメイン116-Vを決定する

V3-2 VLAN識別子、ドメイン116-Vの識別子、及てユーティリティ名をUBNCサーバにに対して送信する

裏筋例2 :

V3-1 接続グループCCの識別子及びユーティリティ名をUBNCサーバに送信する

付録B

ステップM5.0 : リクエストに対するアクセス制御リストの生成ネットワーク110における各ルータについて(I2-3)、またルータの各インターフェースについて(I7)、インターネットと接続されたサブネットが接続グループに属する場合、

A.1 各共用サブネットからのトラフィックを許可する(I8)

A.2 同一の接続グループにおける全てのサブネットからのトラフィックを許可する(I5、I4)

A.3 ネットワーク110における他の全てのサブネットからのトラフィックを拒否する(I1)

A.4 ネットワーク110の外部からのトラフィックを許可する

A.5 ルータにおいてTelnetセッションを開放し、ルータに対して以下を送信する

(1) インタフェースから存在するACL(もし存在すれば)を削除くためのエンド(例えば、非アクセスグループ1)

(2) アクセスリスト

(3) コマンド:

```
interface wlan_e
access-group 1 out
  VLAN 1.4.0.e に対するルータイプエーピー210 のためのアクセス制御リスト
  A.1.1--1. アクセスリスト1許可ip 10.3.4.0 0.0.0.255
  ! 共用サブネット
  A.1.1--2. a. アクセスリスト1許可ip 10.1.2.0 0.0.0.255
  ! 同一のものにおけるサブネット
  ! 企業の接続グループ
  A.1.1--2.b. アクセスリスト1許可ip 10.3.2.0 0.0.0.255
  ! 同一のものにおけるサブネット
  ! 企業接続グループ
  A.1.1--3. アクセスリスト1拒否ip 10.0.0.0 0.255.255.255
  ! ネットワーク1.1.0 における全てのサブネット
  ! 同一の接続グループの外部
  A.1.1--4. アクセスリスト1許可ip 任選
  ! へからのアクセスの許可
  ! ネットワーク1.1.0 の外部
```

付録C
メンテナンスアルゴリズム

接続から接続グループのメンバへのサブネットの変遷
サブネットが1以上のがエイドレスを有する場合、サブネットは接続
グループのメンバに変遷されない。さもなくば、サブネットを接続グループに
付加し、付録Eに示すように、同一の接続グループにおけるサブネットが直接接
続される様々なインターフェースに対するアクセス制御リストを再生成する。
非管理から共用へのサブネットの変遷

共用サブネットのリスト 18 (付録 C) にサブネットを付加する。付録 E に示すように、任職の接続グループにおけるサブネットが接続される各ルータイプアースのアクセス制御リストを再生成する。(サブネットは各ACLに付加され得る。)

共用から非管理へのサブネットの変遷

共用サブネットリストのリスト 18 (付録 C) からサブネットを除去する。付録 E に示すように、任職の接続グループにおけるサブネットが接続される各ルータイプアースのアクセス制御リストを再生成する。(サブネットは各ACLから削除され得る。)

接続グループのメンバからの非管理へのサブネットの変遷

サブネットが 1 を越えるゲートウェイアドレスを有する場合、サブネットは接続グループのメンバに変更されない。そもそもなれば、サブネットを其用サブネット (付録 C) のリスト 18 から除去し、またサブネットを接続グループ (付録 C における 14) に付加する。付録 E に示すように、任職の接続グループにおけるサブネットが接続される各ルータイプアースのアクセス制御リストを再生成する。

接続グループのメンバからの非管理へのサブネットの変遷

接続グループ (付録 C の 15) からサブネットを除去する。付録 E に示すように、同一の接続グループにおけるサブネットが直接接続される各ルータイプアースのアクセス制御リストを再生成する。(サブネットは各ACLから削除され得る。) 付録 E に示すように、サブネットは直接接続されたルータイプアースに対する ACL を除去し、次に (必要ならば) 再生成する。(イニタツフェースに直接接続された他のサブネットが存在しない場合は、ACL は生成されない。別の一単一のサブネット又は複数のサブネットが存在する場合は、適切な ACL が生成される。)

接続グループのメンバからの共用へのサブネットの変遷

接続グループ (付録 C における 15) からサブネットを除去する。サブネットが直接接続されているルータイプアースに対する ACL を除去する。付録 E に示すように、任職の接続グループにおけるサブネットが直接接続されている各ル

—タインタフェースのアタセスサブネットを再生成す。 (サブネットは、ゲループのメソッドとして幾つかのACLから取り除かれるが、其用サブネットとして各ACLに付加される。)

1つの接続グループ（「用」ゲループから別のゲループ（「新」ゲループ）へのサブネットの移行

サブネットを旧ゲループから取り除き、新ゲループ（付録Cの15）に付加する。付録Eによると、古い又は新規の接続グループの例れかににおけるサブネットが直接接続された各ルータイナタブエースのACLを再生成する。

接続グループへの追加エントリ（ポート、MACアドレス、ユーチャ等）の付加

（スルツブM3.0参照）

管理者は、新しいエンティティが属すべ接続グループを指示する。

【0095】

ポート1.6.0 ポートはスイッチ1.2.8に接続され、それはそれを軸体が第2層ドメイン1.1.6の一部である。所定の第2層ドメインにおいて、選択された接続グループは特定のサブネットと接続され、それは、それ自身が特定のVLANと結ばれる。ポートが接続グループに付けられる際に、ステップV1（接続D）が実行され、ポートが第2層ドメインにおける接続グループのメンバであるVLANに配置される。マルチポートモジュールがスイッチに付加される場合のように、或いは全部のスイッチがネットワークに付加される場合のように、通常はポートがグループに付加されることに注目されたい。これらの場合において、新しいポートの全てのセットが、管理者によって選択された接続グループに付加される。次に（もし必要なならば）管理者は一つづつポートの割当を変更することができる。

【0096】

MACアドレス ポートに関する場合のように、特定の第2層ドメインにもじいて、選択された接続グループがサブネット/VLANペアに接続される。各第2層ドメインに対して、ステップV2（付録D）によつて、所定のMACアドレスが指定されたVLANに割当られるよう、全てのスイッチ（又はスイッチの組が次第で、单一の制御スイッチ）が形成される。

【0097】

2-4 付録Dのステップ3を参照。
既存接続グルーピング「B」グルーピングから別のグルーピング「新」グルーピングへの
通信エンティティ（ポート、MACアドレス、エーチ）の移行（ステップM3.0参照）

2-5 ポートはVLAN-capableスイッチ128に接続され、それはそれを自身が第2層ドメインの一部である。第2層ドメインにおいて、新旧の接続グルーピングは特定のサブネットに接続され、それらは、それら自身が特定のVLANに接続される。（新しい接続グルーピングに属する第2層ドメインにおいてサブネットが存在しない場合、変更は行われない。）管理端末124Mは、新しいVLANに対するポートの割当を変更する。

【0098】

2-6 MACアドレス ポートの割合のように、特定の第2層ドメインにおいて、新規の接続グルーピングはサブネット/VLANペアに割り当てる。各第2層ドメインについて、既存のMACアドレスが割り当てられたVLANに割り当てるように、端末124Mが全てのスイッチ（又はMACアドレスの能力が次第で、單一の制御スイッチ）を構成する。特定の第2層ドメインにおける要求された接続グルーピングに對応するサブネットが存在しない場合、第2層ドメインにおけるMACアドレスに割り当てられたラップトグループ又は他のモバイルコンピュータにMACアドレスが割り当てられるために、MACアドレスが第2層ドメインに生じた場合、そこでMACアドレスが発生したときに、それらが通常通り得る全ての動作をとり得る。

【0099】

2-7 付録Dのステップ3を参照。

新規のルータタイミングフェース/ VLAN/サブネットの付加
新規のルータタイミングフェース210が、直接接続されたサブネットを含まない場合（ポートMACアドレスがない場合）、動作は要求されない。さもなくば、インターフェースは以上のデータポートMACアドレス及び対応する直接接続されたサブネットを有する。直接接続された各サブネットについて、
1. サブネットが既に接続グルーピングのメンバーである（從つて、別のルータのイ

ンタフェースに直接接続されている) 場合、サブネットは共用サブネットに変更される。前述の接続グループのメンバのサブネットへサブネットを変更するためのプロセスを参照されたい。

【0100】

2、或いはサブネットが其用又は非管理として既に指定されている場合、動作は要求されない。

【0101】

3、或いはサブネットは新規のサブネットである。サブネットを共用サブネットのリスト18(付録1)に付加する。付録1に示すように、任意の接続グループにおけるサブネットが直接接続された各ルータインターフェースのアカセス制御リストを再生成する。(サブネットは共用サブネットとして各ACLに付加され得る。) サブネットがVLAN…capableスイッチ128を含む第2層ドメインに存在する場合、新規のVLANがドメインごとに生成され、新規のサブネットと接続される。

新規のルータの付加

新規のルータ130は幾つかのインターフェースを有し得る。各ルータインターフェースに対して、新規のルータインターフェースのためにリストされた動作が実行される。

新規のVLAN…capableスイッチの付加

新規のVLAN…capableスイッチ128が第2層ドメインに付加され、そこでは管理接続グループに割当されたサブネットが存在し、またこのグループに対応するVLANが存在する。

【0102】

スイッチが、ポートベースVLAN(port-based VLAN)を実現する場合、スイッチの管理スイッチ及び各ポートにおける全てのポートは、管理接続グループにおけるサブネットに割当される。更に、スイッチはこのサブネットからのIPアドレスに割当られる。例えば、サブネット10.50.3.0/24が、管理グループに割当された第2層ドメインにおけるサブネットである場合、またVLAN3が、サブネット10.50.3.0/24に割当するVLANである場合、管理接続グループに

におけるアドレスに割当てるために、Cisco Catalyst 5000シリーズスイッチのマスクノードにおいて次のようによくマスクドを発行する。

【0103】

```
set interface s0 3 10.50.3.200 255.255.255.0 10.50.3.255
ここでs0は、スイッチの管理スイッチに対する接続子であり、3は、サブネット
ト10.50.3.0/24に対するVLANであり、10.50.3.200は、スイッチの管理スイッ
チに割当されたサブネット10.50.3.200/24におけるIPアドレスであり、255.25
5.255.0は、サブネット10.50.3.0/24に対するサブネットマスクであり、更に10.
50.3.255は障害通信アドレスである。
```

【0104】

スイッチがMACアドレスベースVLANを実現する場合、管理スイッチのMACアドレ
スは、管理接続グループにおけるサブネットに対するVLANに割当てられる。ホ
ームベースVLANの場合のように、スイッチはこのサブネットからのIPアドレスに
割当られる。

【新規の接続グループの付加】

新規の（空の）接続グループは常に付加され得る。サブネットを接続グループ
にどのように付加するかについては前述の通りである。

【画面の簡単な説明】

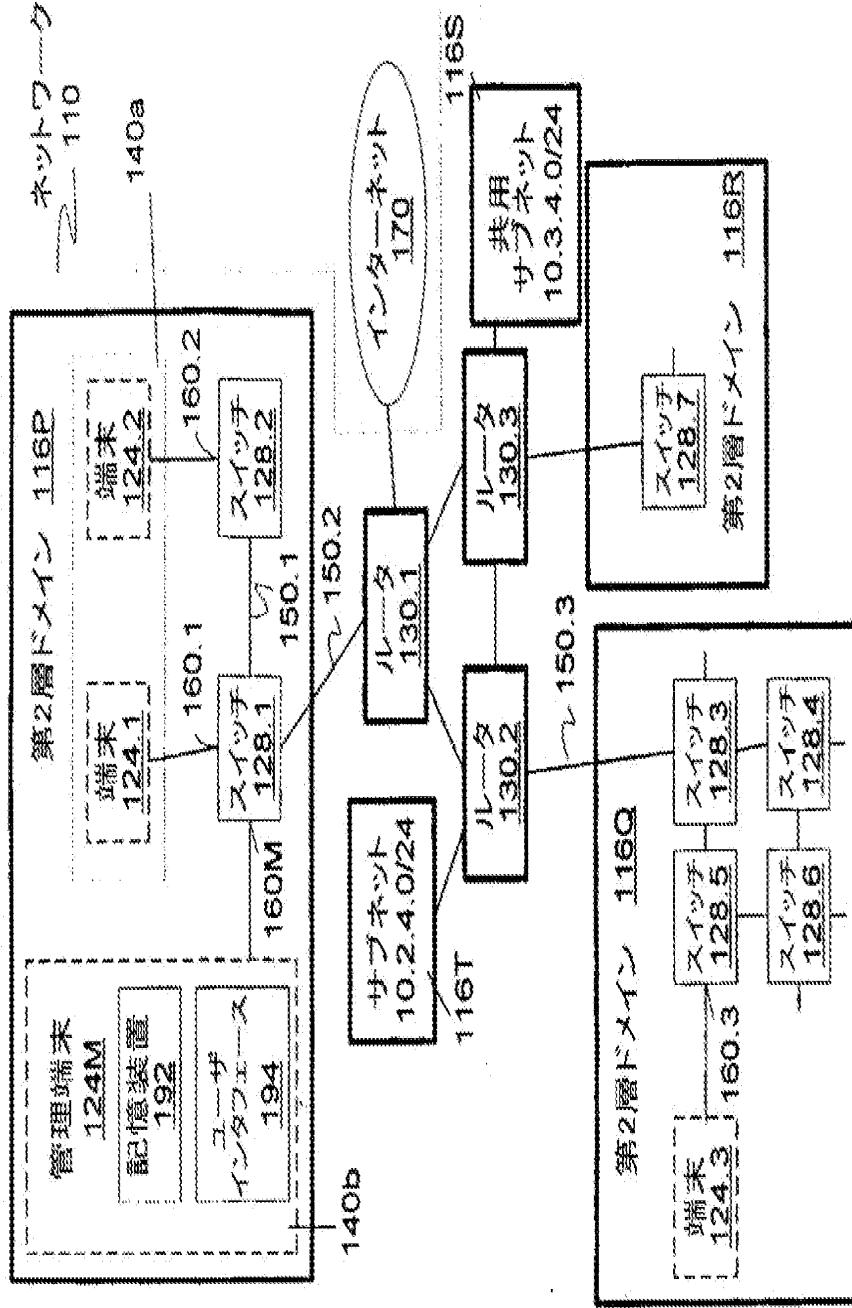
【図1】

本発明により接続を確立したネットワークのアロケーション図である。

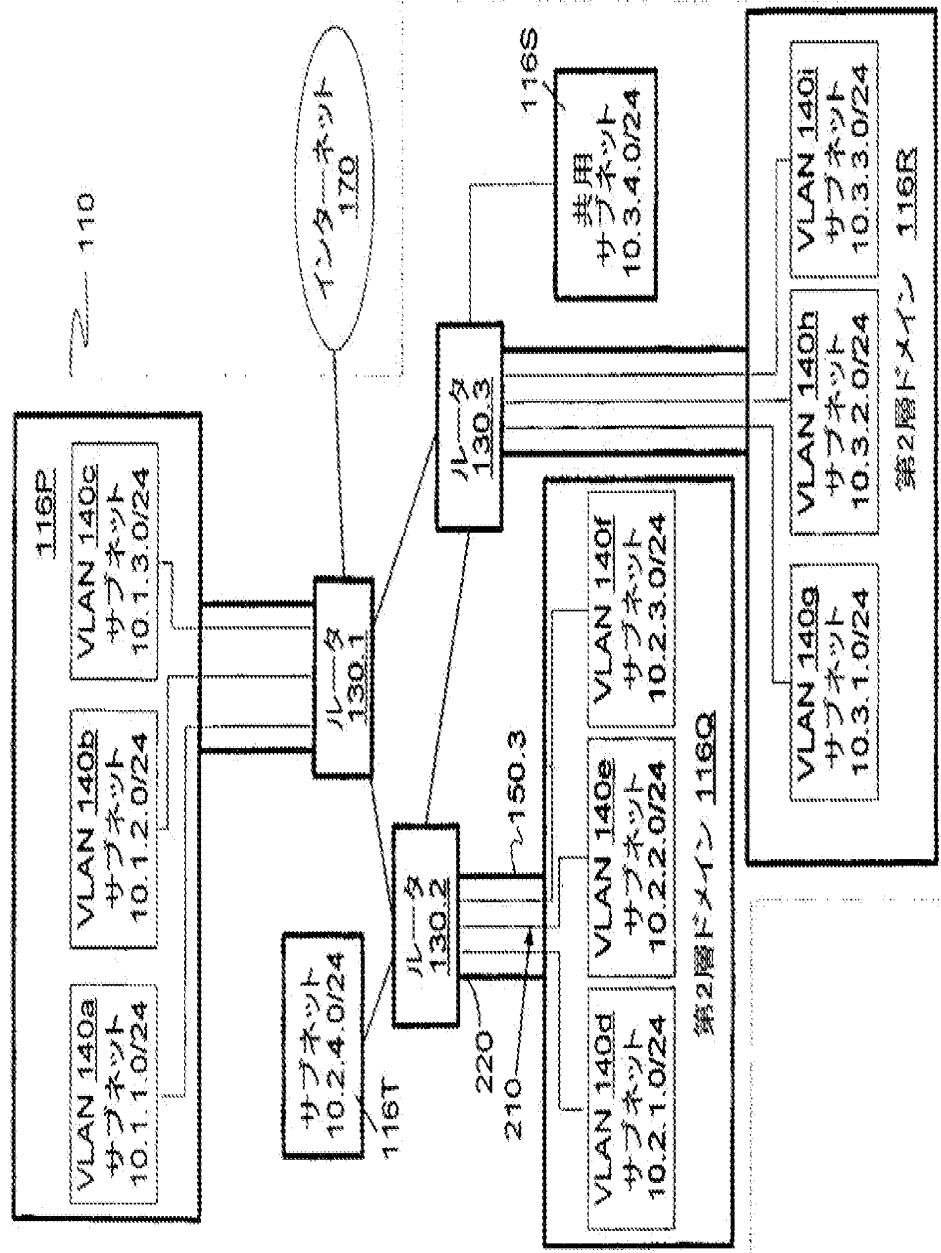
【図2】

図1のネットワークにおけるVLAN及びタグエースを示すプロック線
図である。

三



【図2】



【手続補正書】 特許協力条約第3-4条補正の翻訳文提出書
【提出日】 平成12年4月12日 (2000.4.12)

【手続補正1】

【補正対象書類名】 明細書

【補正対象項目名】 特許請求項の範囲

【補正方法】 変更

【特許請求項の範囲】

【請求項1】

ネットワーク端末をノードチャル間接通信ドメイン (VBDs: 140a乃至140i) に接続するための方法であつて、ネットワーク端末上においてネットワーク端末のユーザを識別する情報を前記ネットワーク端末から受信する過程と、ユーザを識別する情報をから1以上のVBDを含むユーザの属する接続グループを決定する過程と、前記ネットワーク端末が接続される1以上のVBDを決定する過程であつて、前記1以上のVBDが前記接続グループのメンバであるような前記決定過程と、前記ネットワーク端末を前記21以上のVBDに接続するためのコマンドを発行する過程とを含むことを特徴とする方法。

【請求項2】 各VBDが、前記トライックが生じる前記VBDへの情報通信トライックを制限可能なドメイン (1.16P) のサブドメインであり、

前記接続グループが、少なくとも2つのドメインからのVBDを含み、前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含む前記ドメインに属すべき決定されることを特徴とする請求項1に記載の方法。

【請求項3】 各VBDがVLANであり、また前記ネットワーク端末が、前記接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接続されることを特徴とする請求項2に記載の方法。

【請求項4】 ネットワーク端末をノードチャル間接通信ドメイン (VBDs: 140) に接続するための構造体であつて、ネットワーク端末においてネットワーク端末のユーザを識別する情報を前記ネット

トワーカ端末から受信する手段と、
ユーパーを識別する情報から1以上のVBDを含むユーザの属する接続グループを決定する手段と、
前記ネットワーク端末が接続される手段であって、前記
1以上のVBDが前記接続グループのメンバであるような前記決定手段と、
前記ネットワーク端末を前記1以上のVBDに接続するためのコマンドを発行する
手段とを含むことを特徴とする構造体。

【請求項5】 各VBDが、前記トラフィックが生じる前記VBDへの情報通信
トラフィックを制限可能なドメイン(116P)のサブドメインであり、
前記接続グループが、少なくとも2つのドメインからのVBDを含み、
前記ネットワーク端末が接続された1以上のVBDが、前記ネットワーク端末を含
む前記ドメインに基づき決定されることを特徴とする請求項4に記載の構造体。

【請求項6】 各VBDがVLANであり、また前記ネットワーク端末が、前記
接続グループに属するVLAN並びに前記ネットワーク端末を含む前記ドメインに接
続されることを特徴とする請求項5に記載の構造体。

【請求項7】 前記構造体が、(1)所定のコンピュータシステム(112
4M)、及び(2)前記コンピュータシステムにコードされた所定のプログラム
を含み、前記コンピュータシステム及び前記プログラムが、前記決定手段の各々
を含むことを特徴とする請求項4に記載の構造体。

【請求項8】 前記構造体が、所定のコンピュータの讀取の可能な媒体で
あり、そこで各手段が、1以上のコンピュータの命令、コマンド、データの読み取り可
能本データ、又は1以上の命令及びデータの組合せを含むことを特徴とする請求
項4に記載の構造体。

【請求項9】 ネットワークドメイン(116P、116Q、116R、
116S、116T)間のトラフィックの経路を指定する1以上の装置(130
)に対して1以上のアクセス制御リスト(ACLs)を生成するための方法において
、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記
ドメイン間においてどのようなトラフィックが許可及び／又は拒否されるかを決
定し、更に、

サブネットワーク（140a、116T）の1以上上のグループを規定する過程であって、各サブネットワークがネットワークの一部であるか、或いはネットワークドメインの全であり、また各グループに対して、所定のコンピュータシステムに前記グループに属するサブネットワークの識別子を毎まるよう登記過程と、

前記コンピュータシステムが、各グループ内のトライックを許可するためには以上のACLを生成する過程とを含むことを特徴とする方法。

【請求項10】 前記1以上上のACLが異なるグループにおけるサブネットワークのトライックを指すする前記複数のグループを規定する過程を含むことを特徴とする請求項9に記載の方法。

【請求項11】 1以上上の共用サブネットワークの識別子を愛憎する前記コンピュータシステムを更に含む前記方法において、トライックが、前記グループの構成からつににおける各共用ネットワークと任意の別サブネットワークとの間ににおいて許可され、

1以上上のACLによつて、トライックが、前記グループの何れか1つにおける前記共用サブネットワークの何れか1つと任意のサブネットワークとの間ににおいて許可されることを特徴とする請求項9に記載の方法。

【請求項12】 少なくとも1つの前記ドメインが、前記ドメインにおけるトライックを制限することが可能な前記方法であつて、1以上のグループの各々に対して、前記コンピュータシステムが、前記グループ内において許可度び／又は拒否されたトライックを識別するための情報を愛信する過程であつて、前記情報を、制限するトライックにおけるドメインによって使用されるよう前記愛信過程と、

前記情報をによる指定に従つてトライックを許可度び／又は拒否するよう前記コンピュータシステムがトライックを制限可能な各ドメインを構成する過程とを題に含むことを特徴とする請求項9に記載の方法。

【請求項13】 所定のグループ内において許可度び／又は拒否されたトライックを識別するための情報が、1以上の（1）トライックを制限可能な

ドメイン内のトラフィックを各々送信する以上のスイッチ（128）のポート（160）であって、前記グループ内のトラフィックを運ぶための前記ポート（160）と、（2）前記グループに属するエンティティ（124）の物理的アドレスと、更に（3）前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項1.2に記載の方法。

【請求項1.4】 各サブネットワークの識別子が、アドレス又はアドレスレンジであることを特徴とする請求項9に記載の方法。

【請求項1.5】 前記1以上の装置が、IPアドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項9に記載の方法。

【請求項1.6】 ネットワークドメイン（116P、116Q、116R、116S、116T）間のトラフィックの経路を指定する以上の装置（130）に対して以上のアクセス制御リスト（ACLs）を生成するための所定の構造体において、そのような装置にACLが与えられた場合に、前記装置が、前記ACLを用いて前記ドメイン間ににおいてどのようなトラフィックが許可及び／又は拒否されるかを決定し、更に、

各グループ内においてトラフィックが許可されるように、サブネットワーク（140、116）の以上のグループをコンピュータシステムに対して規定する手段であって、各サブネットワークがネットワークードメインの一部であるか、或いはネットワークドメインの全てであり、また各グループに対して、前記グループに属するサブネットワークの識別子をコンピュータシステムによって讀取るための前記規定手段と、

前記コンピュータシステムによって、各グループ内のトラフィックを許可するための以上のACLを生成するための手段とを含むことを特徴とする構造体。

【請求項1.7】 前記構造体が、前記コンピュータシステム（124M）及び該コンピュータシステムにロードされた所定のプログラムを含み、前記コンピュータシステムと前記プログラムとの組合せが、前記規定手段及び生成手段を含むことを特徴とする請求項1.6に記載の構造体。

【請求項1.8】 前記構造体が、前記規定手段及び前記生成手段を実施す

るための命令を含むコンピュータの読み取り可能な媒体であることを特徴とする請求項 1,6 に記載の構造体。

【請求項 1,9】 前記規定手段が複数のグループを規定するときには、前記 1 以上のACIが複数あるグループにおけるサブネットワーク間のトラフィックを拒否することを特徴とする請求項 1,6 に記載の構造体。

【請求項 2,0】 1 以上の其用サブネットワーク (1,16,8) の識別子を前記コンピュータシステムによって読み取るために手段を更に含む前記構造体において、前記グループの何れか一つにおける各共用サブネットワークと他の任意のサブネットワークとの間でトラフィックが許可され、

1 以上の前記ACIによって、前記グループの何れか一つにおける前記共用サブネットワークとの何れか一つと任意のサブネットワークとの間でトラフィックが許可されることを特徴とする請求項 1,6 に記載の構造体。

【請求項 2,1】 少なくとも 1 つの前記ドメインが、前記ドメインにおけるトラフィックを制限可能であるような前記構造体であって、1 以上のグループの各々に対して、前記グループ内における許可及び／又は拒否されたトラフィックを識別するための情報を前記コンピュータシステムによつて読み取るための手段であつて、前記情報が、トラフィックの制限において 1 以上のドメインによって使用されるような読み取り手段と、前記情報による指定に従つてトラフィックを許可及び／又は拒否するようによつて、トラフィックを制限可能な各ドメインを前記コンピュータシステムによつて構成するための手段とを更に含むことを特徴とする請求項 1,6 に記載の構造体。

【請求項 2,2】 所述のグループ内において許可及び／又は拒否されたトラフィックを識別するための情報が、1 以上の (1) トラフィックを制限可能なドメイン内のトラフィックを各々送信する以上のスイッチ (1,2,8) のポート (1,6,0) であつて、前記グループ内のトラフィックを運ぶための前記 1 以上のポート (1,6,0) と、(2) 前記グループに属するエンティティの物理的ポートレースと、更に (3) 前記グループ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項 2,1 に記載の構造体。

【請求項 2,3】 各サブネットワークの識別子が、アドレス又はアドレス

レンジであることを特徴とする請求項 16 に記載の構造体。

【請求項 2-4】 前記 2-4 に、前記 2 以上のおのの装置が、IP アドレスに基づきトラフィックの経路を指定し、また各ドメイン内において、トラフィックが物理的アドレスに基づき端末間で送信されることを特徴とする請求項 16 に記載の構造体。

【請求項 2-5】 様数のドメイン (1-16) を含む所定のネットワークににおける接続を確立するための方法において、

各ネットワーク端末が、第 1 の型のアドレス及び第 2 の型のアドレスを有することが可能であり、

各ドメインにおけるネットワーク端末間のトラフィックが、発先ネットワーク端末の第 2 の型のアドレスを用いて前記発先ネットワーク端末の第 1 の型のアドレスを使用して前記発先ネットワーク端末に送信され、一方でドメイン間においては、前記発先ネットワーク端末の第 2 の型のアドレスを使用してトラフィックが送信され、また制限され、ドメインが單一のサブドメイン内のトラフィックを許可し、一方でサブドメイン間のトラフィックを拒否するように、少なくとも 1 つのドメインが、前記サブドメインにおいて規定されたサブドメイン (1-10) を有するにとが可能であり、更に、

接続グループ CG1 に属するトラフィックを規定する情報 I_NFI をユニピュータシステム (1-2, 4M) に与える過程であつて、前記接続グループ CG1 が、種々のドメインにおいてサブドメインを有するためのものであり、それらの少なくとも 2 つがサブドメインへのトラフィックをそれぞれ制限可能であるような前記過程と、

少なくとも前記接続グループ CG1 について、ドメインが、前記第 2 の型のアドレスを用いることなしに前記第 1 の型のアドレスを使用してトラフィックを送信するときに、前記ドメイン D1 が前記情報 I_NFI によって規定されたトラフィックを許可し、一方でサブドメイン SD1 へのそのようなトラフィックを制限するように、前記コンピュータシステムが、前記接続グループ CG1 におけるサブドメイン SD1 を有する各ドメイン D1 を生成する過程とを特徴とする方法。

【請求項26】 トライフィックを規定する前記情報が、少なくとも1つのグルーパに対して、1以上の(1)單一のドメイン内のトライフィックを各々送信する以上のスピッチ(128)のポート(160)であつて、前記グルーパ内のトライフィックを運ぶための前記ポート(160)と、(2)前記グルーパの端末(124)の物理的アドレスと、更に(3)前記グルーパ内のトライフィックの送信又は受信を許可されたユーザ名との識別子を含むことを特徴とする請求項25に記載の方法。

【請求項27】 各々のドメインを構成する過程が、前記グルーパにおけるサブドメインを有する單一のドメイン内のトライフィックを送信するスピッチについて、(a)前記グルーパのメンバである端末の物理的アドレス間のトライフィックを許可するための、また(b)異なるグルーパのメンバである端末の物理的アドレス間のトライフィックを拒否するための前記スピッチを構成する過程を含むことを特徴とする請求項26に記載の方法。

【請求項28】 複数のドメイン(116)を含む所定のネットワークにおいて、おける接続を確立するための構造体において、各ネットワーク端末が、第1の型のアドレス及び第2の型のアドレスを有することが可能であり、

各ドメインにおけるネットワーク端末間のトライフィックが、最先端トワーク端末の第2の型のアドレスを用いることなしに、前記最先端ネットワーク端末の第1の型のアドレスを使用して前記最先端ネットワーク端末に送信され、一方でドメイソン間ににおいては、前記最先端ネットワーク端末の第2の型のアドレスを使用してトライフィックが送信され、また制限され、トライフィックが單一のサブドメイン内のトライフィックを許可し、一方でサブドメイソン間のトライフィックを拒否するよう、少なくとも1つのドメインが、前記ドメイソンにおいて規定されたサブドメイン(140)を有することが可能であり、更に、

接続グルーパC01に属するトライフィックを規定する情報INFIをコンピュータシステム(124M)によつて受信するための手段であつて、前記接続グルーパC01が、種々のドメインにおいてサブドメイソンを有するためのものであり

、それらの少なくとも2つがサブドメインへのトラフィックをそれぞれ転送可能であるような前記受信手段と、
少なくとも1つの接続グルーブについて、前記接続グルーブのメンバであるサ
ブドメインの識別子を前記コントローラシス템によつて受信する手段と、
少なくとも前記接続グルーブ C₁について、ドメインが、前記第2の型の
アドレスを用いることなしに前記第1の型のアドレスを使用してトラフィックを
送信するときに、前記ドメイン D₁が前記情報 I₁ N₁ F₁によつて規定されたトラ
フィックを許可し、一方でサブドメイン S₁ D₁へのそのようなトラフィックを制
限するように、前記接続グルーブ C₁におけるサブドメイン S₁ D₁を有する各
ドメイン D₁を前記コントローラシス템によつて構成するための手段とを有す
ることを特徴とする構造体。

【請求項 2 9】 トラフィックを規定する前記情報が、少なくとも1つの
グルーブに對して、1以上の(1)単一のドメイン内のトラフィックを各々送信
する以上のスイッチ(128)のポート(160)であつて、前記グルーブ内
のトラフィックを運ぶための1以上の前記ポート(160)と、(2)前記グル
ーブのメンバである端末(124)の物理的アドレスと、更に(3)前記グルー
ブ内のトラフィックの送信又は受信を許可されたユーザ名との識別子を含むこと
を特徴とする請求項 2 8 に記載の構造体。

【請求項 3 0】 前記構造体が、前記コントローラシス템及び該コントロ
ーラシス템にロードされた所定のプログラムを含み、前記コントローラシス
템と該記述プログラムとの組合せが、前記全ての手段を含むことを特徴とする請
求項 2 8 に記載の構造体。

【請求項 3 1】 前記全ての手段を実施するための命令を含むコンピュー
タの読み取り可能な媒体であることを特徴とする請求項 2 8 に記載の構造体。

【請求項 3 2】 各ドメイン内のトラフィックが、端末の物理的アドレス
に基づき端末間で送信され、またドメイン間のトラフィックが、端末の論理的ア
ドレスに基づき経路指定されることを特徴とする請求項 2 8 に記載の構造体。

【手続書類名】 明細書

【補正対象項目名】 0003

【補正方法】 變更

【補正内容】

【0003】

これについて図1及び図2に示す（これらの中には先行技術にはない本発明の幾つかの特徴が示してある）。ネットワーク110は、大規模な組織の相互接続に適する企業ネットワークである。ネットワーク110には、『第2層ドメイン（Layer 2 domains）』116P、116Q、116R、116S、116Tが含まれる（用語「第2層」は、D. Biererらの“NetWare4 for Professionals”（1993）、1-9頁に記載のOSI参照モデルのことを指す）。同一の第2層ドメイン116に属する端末124（例えば、ドメイン116Pにおける端末124-1、124-2）は、それらのACアドレス（第2層アドレス）を用いて互いに通信可能である。MAC（媒体アクセス制御）アドレスは、端末のネットワークインターフェースカード（NIC）に書き込まれた物理的なアドレスであるが、又はNICスイッチの設定によって確定された物理的アドレスである。全てのドメイン116又はその幾つかには、以上のネットワークスイッチ（NICスイッチ）と連携しないが含まれる。各ドメイン116のスイッチ128は、端末のMACアドレスを用いて端末124間でトライアックを送信する。

【手続補正3】

【補正対象書類名】 明細書

【補正対象項目名】 0023

【補正方法】 變更

【補正内容】

【0023】

ユーチャ名によるVLANのメンバーシップの確定については、付録Aに記載されている。（“User-Based Binding of Network Stations to Broadcast Domains”と題するJ. Ekstromの米国特許第5,968,126号（1999年10月19日発行）を参照。これについては、ここで言及することにより本明細書の一部とする。）或る実施例においては、VLAN140が、ポートによつて識別される端末、MACアドレスに

よつて識別される端末、及び／又は二つ以上の名によつて識別される端末を複数有する。

卷之三

INTERNATIONAL SEARCH REPORT

卷之三

INTERNATIONAL SEARCH REPORT

Examination of documents considered to be relevant		Examination of documents considered to be relevant
Cited in the search report as being relevant to the search for prior art		PC1, 45.93/038666
Document	Examination of documents considered to be relevant	Examination of documents considered to be relevant
A	<p>SAUNDERS, S.: "SWITCH PUTS VIRTUAL LANs ON AUTOMATIC PILOT, AGILE'S AUTOMATE SWITCH IS THE FIRST TO AUTOMATE SETUP OF VIRTUAL WORK GROUPS", DATA COMMUNICATIONS, Vol. 23, no. 12, 1 September 1994 (1994-09-01), pages 45/46, XP-000462380, ISSN: 0363-6399</p> <p>the whole document</p>	7, 8, 13, 15, 17, 18, 22-24, 26, 27, 29-32
A	<p>AXHELS, O. H.: "DIFFERING APPROACHES TO VIRTUAL LANs", BUSINESS COMMUNICATIONS REVIEW, December 1993 (1993-12), pages 42-45, XP-000633940</p> <p>abstract</p>	1, 4, 9, 16, 25, 28

(54)

特許2002-313245

INTERNATIONAL SEARCH REPORT

(continued on back page)

Patent document cited in search report		Publication date	Patentability inventor(s)	Publication date
WO 9802821	A	02-01-1998	AU GB	3728497 A 2330285 A
EP 0812036	A	10-12-1997	JP	10056473 A

From PCTDB to International Search Report 09/1998

プロトペーパーの発明

(81) 指定国: EP (AT), BE, CH, CY,
DE, DK, ES, FI, FR, GB, GR, IE,
IT, LU, MC, NL, PT, SE, OA (BE, B
, CF, CG, CL, CM, GA, GN, GW, ML,
MR, NE, SN, TD, TG), AP (CH, GM,
IE, LS, MW, SD, SL, SZ, UC, ZW), E
A (AM, AZ, BY, KG, KZ, MD, RU, T
, TM), AE, AL, AM, AT, AU, AZ, BA
, BB, BG, BR, BY, CA, CH, CN, CU,
CZ, DE, DK, EE, ES, ET, GB, GD, G
E, GA, GM, HR, HU, ID, IL, IN, IS
, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MD, MG, MK, M
N, MW, MX, NO, NZ, PL, PT, RO, RU
, SD, SE, SG, SI, SK, SL, TJ, TM,
TR, TT, UA, UC, UZ, VN, YU, ZA, Z
W

(72) 発明者: エクストロム、ヨセフ・ヨエイ
アメリカ合衆国エタ州84042・ヨンドン
イースト 300サウス 181

(72) 発明者: モス、スティーブン・エス
アメリカ合衆国エタ州84042・リント
ノース 450イースト 298

【発明の範囲】
によつて制限される。